UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/601,374	06/23/2003	David John Craft	AUS920030401US1	7981

46239 7590 06/15/2009

IBM Corporation (PEC)
c/o Patrick E. Caldwell, Esq.
The Caldwell Firm, LLC
PO Box 59655
DALLAS, TX 75229-0655

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
06/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/601,374
Filing Date: June 23, 2003
Appellant(s): CRAFT ET. AL.

Patrick E. Caldwell
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 2-23-2009 appealing from the Office action mailed 10-23-2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

7,082,615	**Ellison et al.**	**9-2000**
6,769,062	**Smeets et al.**	**10-2000**
20020194389	**Worley, JR et al.**	**4-2002**

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

5. Claim **22 - 27, 29 - 36** are rejected under 35 U.S.C. 103 (a) as being unpatentable over **Ellison et al.** (US Patent No. **7,082,615**) in view of **Smeets et al.** (US Patent No. **6,769,062**).

Regarding Claim 22, Ellison discloses a secure processing system, comprising:

a) a main processor unit (MPU) coupled to a processor bus; (see Ellison Figure 1C: host (processor) bus; col. 4, lines 40-45: interface between processors and memory, I/O controller)

b) an attached processor complex (APC) coupled to the processor bus and comprising: a local store configured to store computer instructions and data; (see Ellison col. 4, lines 63-65; col. 3, lines 45-47: load code and data (software), local

store)

c) an attached processor unit (APU) coupled to the local store; wherein the APC is configured to receive commands from the MPU via the processor bus, to store a cryptographic master key (see Ellison col. 4, lines 63-65: APU coupled to host (processor) bus; col. 6, lines 38-42: cryptographic key storage), and to operate in a non-isolated state and an isolated state; (see Ellison col. 4, lines 16-22: partitioned memory, isolated and non-isolated) and

Ellison discloses wherein in response to a LOAD command received from the MPU (see Ellison col. 3, lines 43-45: privileged instruction (such as load command) received and processed by processor), the APC is configured to transition from the non-isolated state to the isolated state (see Ellison col. 4, lines 16-22: based on privileged instruction: partitioned memory, isolated and non-isolated), to transfer a set of computer instructions or data into the isolated section of the local store (see Ellison col. 3, lines 21-25; col. 3, lines 45-49: load code and data to isolated region), and to use the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key. (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption (i.e. key) utilized loading image)

Ellison discloses wherein to partition the local store into a general access section and an isolated section. (see Ellison col. 4, lines 16-22: partition into isolated and non-isolated sections) Ellison does not specifically disclose a general access

section accessible by the MPU and an isolated section accessible only by the APU. However, Smeets discloses:

d) wherein a general access section accessible by the MPU and an isolated section accessible only by the APU. (see Smeets Figure 1 (18: insecure processor); (20: security module); Figure 2 (30: secure processor); col. 2, lines 2-5; col. 2, lines 19-23: one processor secure mode; one processor insecure mode; col. 3, lines 18-20; col. 3, lines 26-28: not a secure processor (main processor); col. 3, lines 58-60: secure processor)

It would have been obvious to one of ordinary skill in the art to modify Ellison to enable the capability for a general access section accessible by the MPU and an isolated section accessible only by the APU as taught by Smeets. One of ordinary skill in the art would have been motivated to employ the teachings of Smeets in order to enable the capability to ensure security based on the widespread usage of digital signatures for electronic commerce and other applications requiring technology for the secure storage of private keys. (see Smeets col. 1, lines 44-50: " *... To ensure the integrity of commercial transactions and to prevent fraud, it is necessary for users to keep their private keys secret. Anyone who has access to the private key of a user can masquerade as that user with complete anonymity. Thus, widespread use of digital signatures for electronic commerce and other applications will require technology for secure storage of private keys.* ... ")

Regarding Claim 23, Ellison discloses the secure processing system as recited in

claim 22, wherein secure processing is performed within the isolated section of the local store of the APC. (see Ellison col. 4, line 63 - col. 5, line 5: secure processing within isolated section, non-secure processing outside)

Regarding Claim 24, Ellison discloses the secure processing system as recited in claim 22, wherein the cryptographic master key stored in the APC is not accessible by the MPU. (see Ellison col. 6, lines 13-18: access restricted to isolated region)

Regarding Claim 25, Ellison discloses the secure processing system as recited in claim 22, wherein the cryptographic master key stored in the APC is unique to the secure processing system. (see Ellison col. 6, lines 64-66: unique cryptographic key (for platform) stored)

Regarding Claim 26, Ellison discloses the secure processing system as recited in claim 22, wherein when the APC is operating in the non-isolated state, the general access section occupies the entire local store. (see Ellison col. 6, lines 13-15: isolated addressing section only setup and defined when in isolated state)

Regarding Claim 27, Ellison discloses the secure processing system as recited in claim 22, wherein when the APC is operating in the isolated state, the APC is configured to respond to an EXIT command received from the MPU by clearing the isolated section of the local store and eliminating the isolated section of the local store,

thereby causing the general access section to occupy the entire local store. (see Ellison col. 5, lines 5-10; col. 3, lines 43-49: privileged instruction (configuration commands), initialize or reset isolated region)

Regarding Claim 29, Ellison discloses the secure processing system as recited in claim 22, wherein the APC further comprises a bus interface unit (BIU) coupled to the processor bus, and wherein local store and the APU are coupled to the BIU. (see Ellison col. 4, lines 40-45: MCH (bus interface unit) coupled to host (processor) bus)

Regarding Claim 30, Ellison discloses the secure processing system as recited in claim 29, wherein the BIU comprises a load/exit state machine (LSEM) configured to store the cryptographic master key. (see Ellison col. 3, lines 21-25; col. 3, lines 45-47: load code and data to isolated region, state machine; col. 6, lines 38-42: store cryptographic key)

Regarding Claim 31, Ellison discloses a method for carrying out secure processing, comprising:

a) providing a main processor unit (MPU), a processor bus, (see Ellison Figure 1C: host (processor) bus; col. 4, lines 40-45: interface between processors and memory, I/O controller) and

b) an attached processor complex (APC), wherein the APC comprises a local store configured to store computer instructions and data and an attached processor

unit (APU) coupled to the local store; (see Ellison col. 4, lines 63-65: attached processor (APU), isolated execution)

d) configuring the MPU to drive a LOAD command on the processor bus in the event secure processing is required; (see Ellison col. 5, lines 5-10; col. 3, lines 43-45: partitioning isolated region, initiation or configuration command)

e) coupling the MPU to the processor bus; (see Ellison Figure 1C: host (processor) bus; col. 4, lines 40-45: interface between processors and memory, I/O controller)

f) configuring the APC to receive the LOAD command via the processor bus, to store a cryptographic master key, and to operate in a non-isolated state and an isolated state; (see Ellison col. 5, lines 5-10; col. 4, lines 16-22: setup isolated and non-isolated states; col. 6, lines 38-42: store cryptographic key)

g) configuring the APC to respond to a received LOAD command by: transitioning from the non-isolated state to the isolated state; (see Ellison col. 5, lines 5-10: configure and setup (APU, LOAD command) isolated state)

i) transferring a set of computer instructions or data into the isolated section of the local store; (see Ellison col. 7, lines 41-43: software to implement; col. 3, lines 21-25; col. 3, lines 45-47: load code or data into isolated region)

j) using the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key; (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption (i.e. key) utilized loading image) and

k) coupling the APC to the processor bus. (see Ellison col. 5, lines 43-46: processor (APC) coupled to memory)

Ellison discloses wherein to partition the local store into a general access section and an isolated section. (see Ellison col. 4, lines 16-22: partition into isolated and non-isolated sections) Ellison does not specifically disclose a general access section accessible by the MPU and an isolated section accessible only by the APU. However, Smeets discloses:

h) wherein a general access section accessible by the MPU and an isolated section accessible only by the APU; (see Smeets Figure 1 (18: insecure processor); (20: security module); Figure 2 (30: secure processor); col. 2, lines 2-5; col. 2, lines 19-23: one processor secure mode; one processor insecure mode; col. 3, lines 18-20; col. 3, lines 26-28: not a secure processor (main processor); col. 3, lines 58-60: secure processor)

It would have been obvious to one of ordinary skill in the art to modify Ellison to enable the capability for a general access section accessible by the MPU and an isolated section accessible only by the APU as taught by Smeets. One of ordinary skill in the art would have been motivated to employ the teachings of Smeets in order to enable the capability to ensure security based on the widespread usage of digital signatures for electronic commerce and other applications requiring technology for the secure storage of private keys. (see Smeets col. 1, lines 44-50)

Regarding Claim 32, Ellison discloses the method as recited in claim 31, wherein the

secure processing is carried out within the isolated section of the local store of the APC. (see Ellison col. 4, line 63 - col. 5, line 5: secure processing within isolated section)

Regarding Claim 33, Ellison discloses the method as recited in claim 31, wherein the cryptographic master key stored in the APC is not accessible by the MPU. (see Ellison col. 6, lines 13-18: access restricted to isolated region)

Regarding Claim 34, Ellison discloses the method as recited in claim 31, wherein the coupling of the MPU and the APC to the processor bus forms a processing system, and wherein cryptographic master key stored in the APC is unique to the processing system. (see Ellison col. 6, lines 64-66: unique cryptography key (for platform) stored)

Regarding Claim 35, Ellison discloses the method as recited in claim 31, wherein when the APC is operating in the non-isolated state, the general access section occupies the entire local store. (see Ellison col. 6, lines 13-15: isolated section only exists when setup and executing)

Regarding Claim 36, Ellison discloses the method as recited in claim 31, further comprising: configuring the APC to respond to a received EXIT command when operating in the isolated state by: clearing the isolated section of the local store; and eliminating the isolated section of the local store, thereby causing the general access section to occupy the entire local store. (see Ellison col. 3, lines 43-45; col. 5, lines 5-10:

command (i.e. instruction) processing, initiate/exit isolated mode; col. 6, lines 13-15: isolated section only exists when setup and executing)

6. Claims **28, 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ellison-Smeets** and further in view of **Worley, JR et al.** (US PGPUB No. **20020194389**).

Regarding Claim 28, Ellison discloses the secure processing system as recited in claim 22, wherein the APC is configured to use the other cryptographic key to decrypt another set of computer instructions or data. (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption (i.e. key) utilized loading image) Ellison does not specifically disclose whereby to authenticate another set of computer instructions or data. However, Worley discloses wherein configured to authenticate another set of computer instructions or data. (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authentication code (instructions or data))

It would have been obvious to one of ordinary skill in the art to modify Ellison-Smeets to enable the capability to authenticate another set of computer instructions or data as taught by Worley. One of ordinary skill in the art would have been motivated to employ the teachings of Worley in order to enable operational control of secure resources without exposing privilege instructions and registers. (see Worley paragraph [0020], lines 16-21: *"... provide a set of secure-platform management services for operational control of hardware resources that neither expose privileged instructions*

and privileged registers of the hardware nor simulate privileged instructions and privileged registers. ... ")

Regarding Claim 37, Ellison discloses the method as recited in claim 31, wherein the configuring the APC to respond to a received LOAD command comprises: configuring the APC to respond to a received LOAD command by:

a) transitioning from the non-isolated state to the isolated state; (see Ellison col. 5, lines 5-10; col. 3, lines 43-45: command processing, isolated region)

c) transferring a set of computer instructions or data into the isolated section of the local store; (see Ellison col. 3, lines 21-25; col. 3, lines 45-47: load code or data into isolated region)

d) using the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic; (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption (i.e. key) utilized loading image) and

Ellison discloses wherein to partition the local store into a general access section and an isolated section. (see Ellison col. 4, lines 16-22: partitioning memory, isolated and non-isolated regions) Ellison does not specifically disclose a general access section accessible by the MPU and an isolated section accessible only by the APU.

However, Smeets discloses:

b) a general access section accessible by the MPU and an isolated section

accessible only by the APU; (see Smeets Figure 1 (18: insecure processor); (20: security module); Figure 2 (30: secure processor); col. 2, lines 2-5; col. 2, lines 19-23: one processor secure mode; one processor insecure mode; col. 3, lines 18-20; col. 3, lines 26-28: not a secure processor (main processor); col. 3, lines 58-60: secure processor)

It would have been obvious to one of ordinary skill in the art to modify Ellison to enable the capability for a general access section accessible by the MPU and an isolated section accessible only by the APU as taught by Smeets. One of ordinary skill in the art would have been motivated to employ the teachings of Smeets in order to enable the capability to ensure security based on the widespread usage of digital signatures for electronic commerce and other applications requiring technology for the secure storage of private keys. (see Smeets col. 1, lines 44-50)

Ellison-Smeets discloses wherein using the other cryptographic key to authenticate or decrypt another set of computer instructions or data. (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption (i.e. key) utilized loading image) Ellison does not specifically disclose whereby to authenticate another set of computer instructions or data.

However, Worley discloses:

e) to authenticate another set of computer instructions or data. (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authentication code (instructions or data))

It would have been obvious to one of ordinary skill in the art to modify Ellison-

Smeets to enable the capability to authenticate another set of computer instructions or data as taught by Worley. One of ordinary skill in the art would have been motivated to employ the teachings of Worley in order to enable operational control of secure resources without exposing privilege instructions and registers. (see Worley paragraph [0020], lines 16-21)

(10) Response to Argument

I. Whether Claims 22-27 and 29-36 are patentable over Ellison et al. (US 7,082,615) ("Ellison") in view of Smeets et al. (US 6,769,062)("Smeets").

A. Applicant argues that for Claims 22 and 31, the referenced prior art does not disclose *"in response to a LOAD command received from the MPU, the APC is configured … to partition the local store into a general access section accessible by the MPC and an isolated section accessible only by the APU". (see Appeal Brief Pages 11, 15)*

Ellison discloses that the isolated region is configured (established) by the execution of an instruction that invokes the isolated operational region. (see Ellison col. 4, lines 63-65; col. 3, lines 43-49: isolated mode instruction is executed; verifies and loads (configures) code or software for isolated operation)

As part of the configuration, Ellison discloses the completion of a task or sequence of steps, performed in response to an instruction or command such as a "LOAD"

command, which initiates the creation of a secure or isolated region. Ellison discloses that the following steps are performed: task loads the ring OS nub into an isolated area; loading application modules including applets into protected pages allocated in the isolated area. (see Ellison col. 3, lines 21-61: load code and data to isolated region), and to use the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store; col. 4, lines 16-22: partitioned into isolated and non-isolated sections)

Smeets discloses that one processor is operational in a secure mode and at the same time a second processor is operational in an insecure mode. (see Smeets Figure 1 (18: insecure processor); (20: security module); Figure 2 (30: secure processor); col. 2, lines 2-5; col. 2, lines 19-23: one processor secure mode; one processor insecure mode; one processor insecure mode; col. 3, lines 18-20; col. 3, lines 26-28: not a secure processor (main processor); col. 3, lines 58-60: secure processor) And, the Ellison discloses that the isolated region is only accessible by a secure processor. (see Ellison col. 6, lines 15-18: access to the isolated area is restricted)

Ellison and Smeets disclose the creation of an isolated region and access restrictions such that only a secure processor can access the isolated region. In addition, an insecure and a secure region exist at the same time.

B. Applicant argues that for Claims 22 and 31, the referenced prior art *"teaches away"* from the claims. *(see Pages 14 of Appeal Brief)*

Ellison and Smeets do not teach away from the creation of an isolated region. Ellison and Smeets are in the same field of endeavor as Applicant's claimed invention, which is the creation of a secure or isolated execution environment. (see Ellison col. 2, lines 41-46: isolated execution environment; col. 4, lines 16-22: partitioned memory, isolated and non-isolated; see Smeets col. 2, lines 2-5: secure (isolated) and non-secure devices for performing cryptographic calculations) The prior art references do not discredit, or discourage the creation of a secure or isolated region. (MPEP 2145[R.3].X.D.1)

II. Whether Claims 28 and 37 are patentable over Ellison and Smeets in view of Worley Jr. et al. (US PGPUB 2002/0194389)("Worley").

Applicant argues that for Claims 28 and 37, *"Worley does not show an isolated section accessible only by the APU that is partitioned in response to a LOAD command". (see Pages 14, 15 of Appeal Brief)*

Worley is not used to disclose *"an isolated section accessible only by the APU in response to a LOAD command".* Worley is used to disclose authenticating another set of instructions using a cryptographic key.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(12) Conclusion

For the above reasons, it is believed that the rejections should be sustained.

/Carlton V. Johnson/

Examiner, Art Unit 2436

Conferees:

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435